

# **IN THE CLAIMS:**

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~striketrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND the claims in accordance with the following:

1. (Currently Amended) An authentication information processing method comprising:
    - acquiring apparatus information of a user apparatus requesting a log-in;
    - determining a log-in procedure to be applied to the user apparatus on the basis of the apparatus information;
    - accepting a log-in operation from the user apparatus;
    - judging, based on the determined log-in procedure and on the accepted log-in operation, whether the log-in from the user apparatus is permitted or not;
    - storing a last log-in time from the user apparatus with the last log-in time related to the apparatus information; ~~and~~
    - storing security level with the last log-in date related to the security ~~level~~, level;
    - storing an accumulated log-in count from the user apparatus with the log-in count related to the apparatus information; and
    - determining a security level for the user apparatus by referring to at least an accumulated log-in count.
- wherein in determining the log-in procedure, the log-in procedure is determined by raising the security level when a period longer than a predetermined period has elapsed since the last log-in time,
- wherein in determining the log-in procedure, the log-in procedure is determined by lowering the security level when a number of days since the last log-in date is smaller than a predetermined small number of days.

wherein in determining the log-in procedure, the log-in procedure is determined in accordance with the accumulated log-in count and the security level, and the security level is lowered when formal log-in procedure is repeated.

2. (Cancelled).

3. (Cancelled).

4. (Cancelled).

5. (Currently Amended) An authentication information processing device, comprising:

an apparatus information acquiring module ~~acquiring~~ configured to acquire apparatus information of a user apparatus requesting a log-in;

a log-in procedure determining module ~~determining~~ configured to determine a log-in procedure to be applied to the user apparatus on the basis of the apparatus information;

a log-in accepting module ~~accepting~~ configured to accept a log-in operation from the user apparatus;

a log-in judging module ~~judging~~ configured to judge, based on the determined log-in procedure and on the accepted log-in operation, whether the log-in from the user apparatus is permitted or not;

a last log-in time storing module ~~storing~~ configured to store a last log-in time of the user apparatus, the last log-in time being related to the apparatus information; and

a security level storing module ~~storing~~ configured to store a security level with a last log-in date related to the security level, ~~level~~;

an accumulated log-in count storing module configured to store an accumulated log-in count from the user apparatus with the accumulated log-in count related to the apparatus information; and

a security level determining module configured to determine a security level for the user apparatus by referring to at least an accumulated log-in count,

wherein the log-in procedure judging module determines the log-in procedure by raising the security level when a period longer than a predetermined period has elapsed since the last log-in time,

wherein in determining the log-in procedure, the log-in procedure is determined by lowering the security level when a number of days since the last log-in date is smaller than a predetermined small number of days,

wherein the log-in procedure judging module determines the log-in procedure in accordance with the accumulated log-in count and the security level, and the security level is lowered when formal log-in procedure is repeated.

6. (Cancelled).

7. (Cancelled).

8. (Cancelled).

9. (Currently Amended) A storage medium that stored an authentication information processing program making a computer to execute a process authentication information, comprising:

acquiring apparatus information of a user apparatus requesting a log-in;

determining a log-in procedure to be applied to the user apparatus on the basis of the apparatus information;

accepting a log-in operation from the user apparatus; and

judging, based on the determined log-in procedure and on the accepted log-in operation, whether the log-in from the user apparatus is permitted or not;

storing a last log-in time from the user apparatus with the last log-in time related to the apparatus information; and

storing security level with the last log-in date related to the security level, level;

storing an accumulated log-in count from the user apparatus with the log-in count related to the apparatus information; and

determining a security level for the user apparatus by referring to at least an accumulated log-in count.

wherein in determining the log-in procedure, the log-in procedure is determined by raising the security level when a period longer than a predetermined period has elapsed since the last log-in time,

wherein in determining the log-in procedure, the log-in procedure is determined by

lowering the security level when a number of days since the last log-in date is smaller than a predetermined small number of days,

wherein in determining the log-in procedure, the log-in procedure is determined in accordance with the accumulated log-in count and the security level, and the security level is lowered when formal log-in procedure is repeated.

10. (Cancelled).

11. (Cancelled).

12. (Cancelled).